

47 Trinity Avenue
Atlanta, Georgia 30334

Phone: 404.463.2300
Fax: 404.463.2380



Georgia Technology Authority
www.gta.georgia.gov



SONNY PERDUE

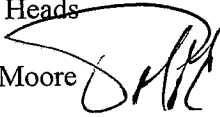
Governor

PATRICK MOORE

Executive Director and
State Chief Information Officer

February 19, 2009

MEMORANDUM

TO: Agency Heads
FROM: Patrick Moore 
RE: Virus infections of state computers on the rise

The U.S. Department of Homeland Security (DHS) reports that there were more incidents of computers becoming infected by viruses and related software in July 2008 than in the previous 12 months combined. DHS is reporting the potential compromise of 3 to 5 State of Georgia computers per day. Just today, we received a report from DHS indicating over 350 sites are infected with a virus capable of accessing and distributing state data.

Your agency may be at risk. Given this increasing threat level, GTA will escalate security-related threats to agency heads after one business day unless the Senior Agency Information Security Officer responds to the initial notification. This is to ensure that your agency has received and understood the notification, and so that GTA may collect information designed to improve the state's overall security posture.

In March 2008, Governor Perdue issued an executive order calling for annual agency-level information security reports. Also during that month, GTA launched the state's new security program modeled after the federal program created by the Federal Information Security Management Act (FISMA). While these two actions established the standards for security and the method of measurement, agencies are still responsible for implementing required security controls.

It is critical that all state agencies take appropriate and timely steps to protect their Windows-based desktop and server environments. The appendix to this memo includes those recommended steps.

If you or your staff have any questions regarding this memo or information security in general, please contact Mark Reardon, Chief Information Security Officer, at 404-657-0818 or email gta-ois@gta.ga.gov.

cc: Mr. Jim Lientz, Chief Operating Officer
Mr. Tommy Hills, Chief Financial Officer

GTA's Vision:

To provide exemplary customer service; To enable business solutions for Georgia's state government; To lead change for Georgia's state government

Appendix

To underline the importance of this process, here are some facts about one virus-like program called Conficker:

- On August 8, 2006, Internet Security Systems (ISS) updated its intrusion prevention (IPS) product line to protect against attempts to exploit an underlying flaw in Windows.
- On October 23, 2008, Microsoft released a critical emergency patch for Windows to remove this underlying flaw.
- On November 21, 2008, Conficker was discovered on the Internet. It can only infect a system missing the new patch and that is not protected by the ISS IPS product line.
- On November 21, 2008, most major antivirus vendors updated their products to protect against Conficker. It was estimated that half a million computers had been infected.
- On November 26, 2008, at DHS's request, GTA asked all state agencies to update their antivirus products and conduct complete scans of all Windows systems.
- On January 26, 2009, 10,000,000 computers are infected with Conficker. Unfortunately, some belong to the State of Georgia.
- The 10,000,000 Conficker infections represent approximately 4% of the botnet-infected systems worldwide.

Recommended steps for agency protection of their Windows servers, desktops and laptops:

1. Have a monthly patching program that includes a process for implementing emergency patches when warranted. Most malware attacks exploit known vulnerabilities. Research has shown that while patching is necessary, a monthly patching regime would avoid over 95% of all known exploits.
2. All operating systems should have antivirus and intrusion prevention programs that can protect against the latest malware. These programs should be patched or updated at least monthly. A good antivirus program is able to identify known malware and block its installation or execution. A good intrusion prevention program is able to identify and block most attacking programs based on the program's inappropriate behavior. The combination is strong protection against all attacks.
3. Have an approved list of applications that can run on any system and periodically audit systems to check for compliance. Malware often masquerades as another type of program so unapproved software has the potential for being malware.
4. Only allow dedicated system administrator accounts the ability to install programs and remove or disable default systems accounts that come with the system. Those administrators should follow standard administrative practices to avoid distributing malware to systems through thumb drives, writeable CDs/DVDs, or other media.
5. Use hard to guess (complex) passwords on your system accounts. Many of the newer malware are able to circumvent weak administrator passwords and gain privileged access to the system or network.